**Quelques tabous & totems de la sécurité revisités…**

**Par Mauro Israel – coordinateur du Cercle de la Sécurité et des Systèmes d'Information**

***Les frères « Térieur » : Alain et Alex***

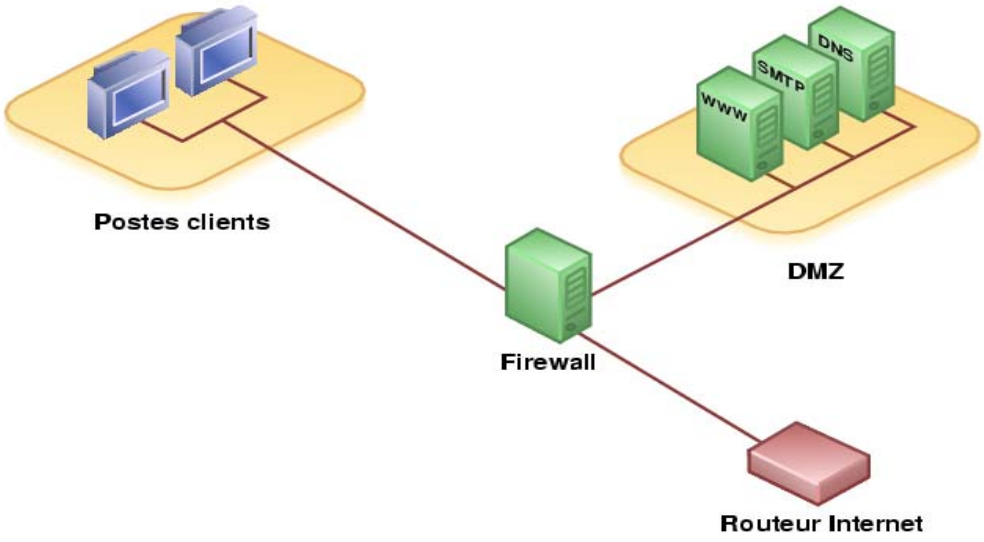
**Tabou numéro 2 : Le firewall ne bloque pas TOUTES les attaques…**

Le deuxième plus grand tabou de toute l'industrie de la sécurité, (après celui des anti-virus discuté dans l'article précédent) est de ne pas divulguer le fait que **les firewalls** (sans autre dispositif supplémentaire) **ne bloquent qu'une partie des attaques des pirates,** et ceci par construction. Autrement dit, croire qu'un simple firewall protège complètement votre système informatique est un leurre.

**Petit historique des firewalls.**

Les firewalls ont été conçus initialement pour bloquer les attaques venant d'Internet en appliquant une règle simple et ceci pour toutes les couches du modèle OSI, depuis le physique jusqu'aux protocoles applicatifs : *« Tout ce qui n'est pas explicitement autorisé est interdit ».* Cette règle est paramétrée sous forme de liste explicite et chaque paquet qui rentre ou sort du réseau, est filtré par cette passerelle qui délimite donc « l'intérieur » et « l'extérieur ». La « frontière » entre le LAN (réseau local interne) et le WAN (réseau externe) ou Internet. On ajoute donc uniquement les règles qui permettent de fonctionner correctement, par exemple, « pour tous les ordinateurs du réseau local, autoriser le surf sur Internet (http port 80) et le surf chiffré (http port 443). S'ensuit une série de règles qui permettent toutes les activités du site. La dernière règle est toujours *« tout le reste non prévu est bloqué ».* Donc si un intrus de l'extérieur tente de rentrer sur le port 12345 cela est refusé, sauf si un utilisateur interne a initié la connexion…

**La DMZ**




*Source Wikipedia*

On a alors inventé des zones démilitarisées (DMZ) sortes de sas entre l'intérieur et l'extérieur, qui permettent de joindre certaines machines depuis l'extérieur, notamment les serveurs web ou email. Cette DMZ est donc séparée par construction à la fois du réseau local et d'internet et tous les flux passent toujours par le firewall. Une situation idéale donc : on peut à la fois aller surfer sur internet de manière protégée et également recevoir des « visiteurs » qui sont cantonnés à la DMZ. Oui, idéale, sauf si le serveur est contaminé, voire « zombifié », c'est-à-dire que grâce à un exploit de contamination, un pirate prend la main sur un serveur de la DMZ et par « rebond » rentre dans le réseau local… Cela est-il possible ? Oui, si le serveur « cible » présente des vulnérabilités. Ces vulnérabilités sont facilement analysables de l'extérieur avec un scanner de vulnérabilités. Le plus connu étant Nessus. La première action d'un apprenti pirate est donc de « scanner » toute la journée automatiquement des plages d'adresses IP publiques (dont votre DMZ) et de récupérer le soir, en revenant du collège ou du lycée, les machines qui sont vulnérables à telle ou telle attaque. Comment une machine est-elle encore vulnérable à une attaque malgré le firewall ?

**Patchez ! Patchez ! Patchez !**

La machine en question souffre de l'absence de l'installation de patches (correctifs de sécurité), publiées par l'éditeur du système d'exploitation ou du firmware dans le cas d'un boitier dédié. Pour chaque exploit il existe un patch correspondant chez l'éditeur, sauf ce qu'on appelle les *« zero day »,* c'est-à-dire que le correctif n'existe pas encore, alors que l'exploit a été publié sur Internet. Le « travail » des pirates est considérablement plus simple qu'il y a quelques années, car des sites comme *« Metasploit »* publient les scripts d'attaque pour telle ou telle vulnérabilité. Il suffit donc de scanner des plages publiques, puis d'attaquer le site non patché avec l'exploit correspondant… C'est tellement simple et sans aucun intérêt « informatique ». Mais l'intérêt est ailleurs…

La question est donc : combien de serveurs publics dans les DMZ ne sont pas complètement « patchés » ? Des centaines de milliers ! Pourquoi ? Pour plusieurs « bonnes raisons » : la première qui est invoquée – et tout à fait légitime – est que l'application qui tourne sur ce système-là est figée à une version qui n'est garantie par l'éditeur ou le développeur que sur « Windows NT 4.0 ». Or Microsoft ne publie plus les patches pour ce système depuis plusieurs années, mais il est toujours présent dans l'inventaire des entreprises pour cette raison là. Ces systèmes « non patchables » sont donc en grand danger. Il faut les retirer de la DMZ ou faire une montée de version ou trouver une autre solution…

Une deuxième raison –légitime également- est le cas des bases de données : Si on patche le moteur d'une base de données, il se peut que le système ne redémarre pas correctement, voire se plante ou que les données soient perdues ou désindexées, ce qui serait une catastrophe pour l'entreprise. En effet l'impact sur un système de bases de données est autrement plus important que le simple patch sur un poste de travail, ou même une série de postes de travail. Les « DBA », administrateurs de bases de données sont donc très réticents à *patcher* car ils redoutent un déni de service ou une réaction imprévisible avec l'applicatif qui tourne sur la base de données en question.

Or il s'avère que les attaques se sont décalées vers les bases de données, car notre apprenti pirate se rend compte que les systèmes d'exploitation et les réseaux sont de mieux en mieux protégés, alors que de nombreuses bases de données sont restées dans leur état d'installation initiale, donc vulnérables.

De nombreux éditeurs de bases de données ont emboité le pas de Microsoft avec Windows Update (qui fonctionne aussi pour Sql Server) et proposent des patches, depuis plusieurs années, comme le cas d'Oracle avec ses « CPU », « Critical Patch Updates » depuis 2005. Or force est de constater que ces patches ne sont pas appliqués dans de nombreux cas, ce qui conduit souvent aux « exploits » dont se fait echo la presse : *« Des milliers de numéros de cartes bancaires dérobés »* ou *« des milliers de données privées divulguées sur Internet »*…

http://v9.update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=fr

http://www.oracle.com/technology/deploy/security/alerts.htm

**Pirate de base de données : mode d'emploi.**

Comment cela est-il possible, malgré le firewall ? On l'a compris, l'absence de patches sur la base de données rend possible un exploit qui traverse le firewall en toute impunité et la base est dévoyée. Comment cela fonctionne-t-il dans le détail ? En fait, dès qu'un patch est publié par l'éditeur, les sites de hacking spécialisés se précipitent sur le code du patch et procèdent à un « re-engineering » du code binaire vers le code source. Ainsi ils comprennent ce qui est corrigé et par déduction quelle est la faille qui est colmatée, puis en déduisent également le code d'attaque qui exploite cette faille. Ainsi de manière ironique, **la publication du patch a permis de créer le code d'attaque,** sauf pour les quelques « génies » qui avaient trouvé le problème… Donc, après publication du patch la situation devient la suivante : au bout de quelques jours, n'importe quel pirate de base peut lancer une attaque gagnante sur un système non patché, alors qu'avant la publication du patch, cette attaque était réservée à une « élite »… La boucle est bouclée, il suffit de scanner toutes les machines présentes sur Internet et on peut attaquer toutes celles non patchées…

Quelle est la situation réelle face aux patches ? Par exemple, lors de la faille des DNS de juillet 2008, appelée faille « Kaminsky » du nom de son découvreur, les patches ont été publiés pour la première fois de concert pour tous les éditeurs concernés, clients ou serveurs de noms de domaine. Plus d'un an après, où en est-on ? Près de 30% des serveurs BIND et autres WINS-DNS ne sont toujours pas patchés, rendant toujours possible l'attaque, dévoilée par le re-engineering du patch à peine 11 jours après avoir dévoilé l'exploit…

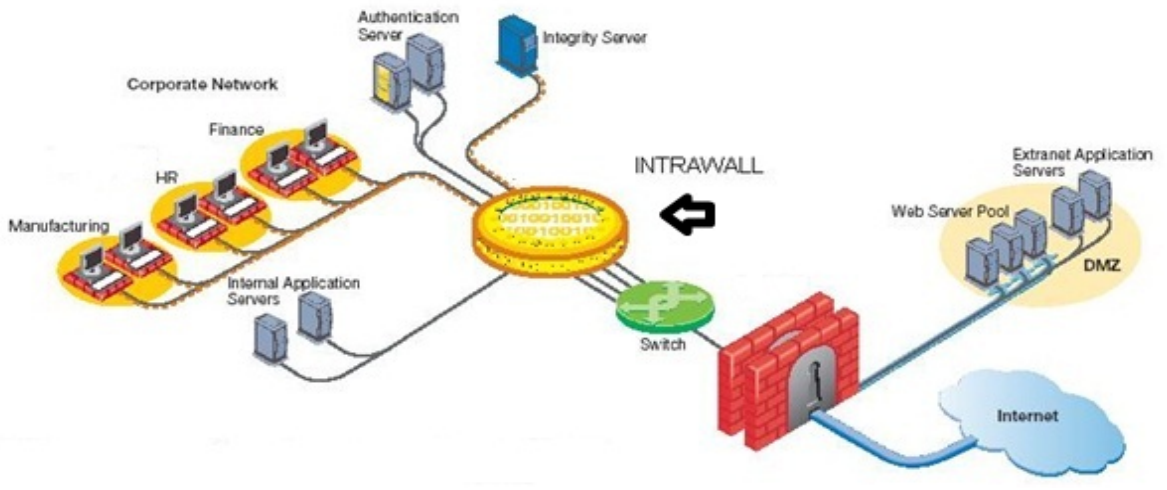
En fait on est en présence aujourd'hui de failles structurelles de l'Internet qui n'a pas du tout été conçu au départ pour être sécurisé, mais pour interconnecter des machines hétérogènes entre elles. Ces failles structurelles nécessitent, comme l'a indiqué avec regrets, Vinton Cerf l'un des créateurs d'Internet, de repenser notamment des fonctions de sécurité au sein même du protocole. L'arrivée d'IP V6 va certainement contribuer à améliorer la situation du côté des réseaux, mais pour

les applications et les bases de données, le slogan « Patchez-Patchez-Patchez !» sera toujours d'actualité dans plusieurs années.

**Floutage de l'intérieur et de l'extérieur.**

Et puis il y a eu la montée en puissance des ordinateurs portables. Certaines entreprises équipent systématiquement leurs utilisateurs avec des ordinateurs portables, mêmes s'ils sont en fait appelés à ne jamais bouger de leur bureau… Cette masse d'ordinateurs nomades sont quand même souvent emportés à la maison ou en déplacement et se connectent alors à Internet sans la protection perimétrique du firewall. Si un logiciel malicieux parvient à s'installer lors de ce moment, lors du rebranchement du portable sur le réseau de l'entreprise, **celui-ci se trouve alors à l'intérieur du réseau et peut contaminer à loisir le reste du réseau**. De même avec des **clefs USB** qui sont très utilisées pour transporter des fichiers entre ordinateurs et **sont un vecteur de contamination important**. La protection des accès distants par le chiffrement, rend certes difficile à intercepter les flux entre un nomade et le réseau de l'entreprise, mais permet à une menace de s'introduire de manière « encapsulée » dans le réseau, puisque le flux est justement chiffré y compris pour le firewall.

Ce pauvre firewall ne suffit donc plus à protéger le réseau de l'entreprise, car il est comme une coquille d'œuf : relativement efficace pour empêcher les attaques de l'extérieur, mais dès que l'on est à l'intérieur de l'œuf, c'est « tout mou », et la séparation entre le « blanc » et le « jaune » est tout à fait ténue. Alors, comment se protéger contre ces types d'attaques ? **En ajoutant au cœur du réseau** un autre type de firewall dit « comportemental », - que j'appelle **un « intrawall »-** qui laisse passer tous les flux par défaut au contraire du firewall classique, mais qui **repère un comportement suspect d'une machine et qui la bloque**, prévient l'administrateur et la met en quarantaine. Par exemple, une machine qui tente d'envoyer des *scans* de ports sur toutes les machines du réseau, puis qui cherche à recopier un fichier exécutable en utilisant les partages de réseau local est suspecte (sauf s'il s'agit d'une sonde parfaitement connue des administrateurs). Cette machine est repérée et bloquée -ce qui ne nettoie pas le logiciel malicieux- mais qui empêche sa diffusion.




*Source Checkpoint*

**Epilogue sur les frères « Térieur ».**

Avec des « frontières » de plus en plus floues entre l'intérieur et l'extérieur, le firewall ne peut protéger (vaillamment) que le périmètre, mais ne peut pas protéger de certaines attaques.

Voilà : du « tabou » sur les firewalls nous arrivons à un « totem » de la sécurité informatique : **L'application systématique des correctifs de sécurité**…

Nous avons atteint un autre « totem » : **La protection des postes nomades et des accès distants**.

Un dernier totem: **Le contrôle des clefs USB et autres supports de mémoire amovibles…**

Au fait, qui croira encore aux statistiques sur le pourcentage de « menaces internes » versus « menaces externes » ; ça ne veut plus rien dire ! L'intérieur et l'extérieur ne font qu'un. Et **nous sommes,** qu'on le veuille ou non**, entrés dans l'ère du *« cloud »*** : le nuage d'Internet.

La suite, pour le prochain tabou, traitera du *« login-passoire » …*

Mauro Israel